

## CLAIMS

What is claimed is:

- 1 1. A method of automatically generating an updated key value for a segment of  
2 keystream for use in a cipher, with forward security, the method comprising the  
3 computer-implemented steps of:  
4 receiving a location value that identifies a location of the segment within the  
5 keystream;  
6 generating the updated key value corresponding to the identified segment and based  
7 on a current key value with forward security and without relying on a key  
8 management process for providing such forward secrecy; and  
9 wherein determining another key value based on the current key, the updated key, and  
10 state values that are stored during the generating is computationally infeasible.
- 1 2. A method as recited in Claim 1, wherein generating the updated key value further  
2 comprises:  
3 creating and storing values in a memory that correspond to a logical tree, wherein the  
4 tree represents the keystream, wherein each leaf node of the tree represents a  
5 particular keystream segment associated with a discrete location in the  
6 keystream, and wherein an order of each leaf node in pre-order traversal of the  
7 tree corresponds to a sequential order of all keystream segments.
- 1 3. A method as recited in Claim 2, wherein generating the updated key value further  
2 comprises:  
3 creating and storing an ordered plurality of data elements, wherein each of the data  
4 elements is identifiable by a node value that is associated with a unique leaf  
5 node or intermediate node in the tree, and wherein each of the data elements  
6 stores a keystream segment.

- 1 4. A method as recited in Claim 3, wherein generating the updated key value further  
2 comprises generating the key value based on the steps of:  
3 selecting a highest-ordered element from among the plurality of data elements;  
4 if the selected element is not associated with a leaf node, then:  
5 storing, in a new highest-ordered element among the plurality of data  
6 elements, a first new key value that is determined by applying a first  
7 pseudo-random function to the selected element;  
8 generating a second new key value by applying a second pseudo-random  
9 function to the selected element.
- 1 5. A method as recited in Claim 4, wherein generating the updated key value further  
2 comprises generating the updated key value based on the steps of:  
3 returning, as the updated key value, a segment of the keystream associated with the  
4 node identified in the selected next node value when such node is a leaf node;  
5 returning, as the key value that is generated, a segment of the keystream associated  
6 with the second new node value when the node identified in the selected next  
7 node value is not a leaf node.
- 1 6. A method as recited in Claim 3, wherein generating the updated key value further  
2 comprises generating the key value based on the steps of:  
3 determining a current location value;  
4 identifying an internal node of the tree having a highest node number that is an  
5 ancestor of a first node corresponding to the received location value and of a  
6 second node corresponding to the current location value;  
7 determining a path from the identified internal node to the first node;  
8 traversing the path while applying a first pseudo-random key updating function to the  
9 then-current key value during each leftward downward transition and applying  
10 a second pseudo-random function during each rightward downward transition.

- 1 7. A method as recited in Claim 6, wherein generating the updated key value further  
2 comprises generating the updated key value based on the steps of:  
3 storing, in a new highest-ordered element among the plurality of data elements, each  
4 new key value that is generated as part of applying the first and second  
5 pseudo-random functions;  
6 generating, as the updated key value, the new key value that stored in the highest-  
7 ordered element among the plurality of data elements, when the first node is  
8 reached in traversing the path.
- 1 8. A method as recited in Claim 2, wherein each edge of the tree is associated with a  
2 distinct pseudo-random function that, when applied to a current key, results in  
3 generating a new updated key.
- 1 9. A method as recited in Claim 2, wherein each edge leading leftward and downward  
2 from a first node to a second node is associated with a first pseudo-random key  
3 updating function, and wherein each edge leading rightward and downward from the  
4 first node to a third node is associated with a second pseudo-random key updating  
5 function.
- 1 10. A method as recited in Claim 6, wherein each of the pseudo-random functions  
2 receives, as input, a first keystream segment and generates, as output, a second  
3 keystream segment based on updating the first keystream segment in a pseudo-  
4 random manner, such that determining the first keystream segment based on the  
5 second keystream segment is computationally infeasible.
- 1 11. A method as recited in Claim 1, further comprising the steps of distributing the  
2 updated key value to each member of a multicast group for use in secure  
3 communications among the multicast group.

1 12. A method of automatically generating an updated key value for a segment of  
2 keystream for use in a cipher, with forward security, the method comprising the  
3 computer-implemented steps of:  
4 receiving a location value that identifies a location of the segment within the  
5 keystream;  
6 generating the updated key value corresponding to the identified segment and based  
7 on a current key value with forward security and without relying on a key  
8 management process for providing such forward secrecy;  
9 wherein determining another key value based on the current key, the updated key, and  
10 state values that are stored during the generating is computationally infeasible;  
11 creating and storing values in a memory that correspond to a logical tree, wherein the  
12 tree represents the keystream, wherein each leaf node of the tree represents a  
13 particular keystream segment associated with a discrete location in the  
14 keystream, and wherein an order of each leaf node in pre-order traversal of the  
15 tree corresponds to a sequential order of all keystream segments;  
16 creating and storing an ordered plurality of data elements, wherein each of the data  
17 elements is identifiable by a node value that is associated with a unique leaf  
18 node or intermediate node in the tree, and wherein each of the data elements  
19 stores a keystream segment;  
20 selecting a highest-ordered element from among the plurality of data elements;  
21 if the selected element is not associated with a leaf node, then:  
22 storing, in a new highest-ordered element among the plurality of data  
23 elements, a first new key value that is determined by applying a first  
24 pseudo-random function to the selected element;  
25 generating a second new key value by applying a second pseudo-random  
26 function to the selected element;  
27 returning, as the updated key value, a segment of the keystream associated with the  
28 node identified in the selected next node value when such node is a leaf node;

29           returning, as the key value that is generated, a segment of the keystream  
30           associated with the second new node value when the node identified in  
31           the selected next node value is not a leaf node;  
32       determining a current location value;  
33       identifying an internal node of the tree having a highest node number that is an  
34           ancestor of a first node corresponding to the received location value and of a  
35           second node corresponding to the current location value;  
36       determining a path from the identified internal node to the first node;  
37           traversing the path while applying a first pseudo-random key updating  
38           function to the then-current key value during each leftward downward  
39           transition and applying a second pseudo-random function during each  
40           rightward downward transition;  
41       storing, in a new highest-ordered element among the plurality of data elements, each  
42           new key value that is generated as part of applying the first and second  
43           pseudo-random functions;  
44           generating, as the updated key value, the new key value that stored in the  
45           highest-ordered element among the plurality of data elements, when  
46           the first node is reached in traversing the path.

- 1   13.   A method of enciphering a plaintext using at least an updated key value for a segment  
2       of a keystream, with forward security, the method comprising the computer-  
3       implemented steps of:  
4       receiving a plaintext segment;  
5       receiving a location value that identifies a location of the plaintext segment within a  
6           plurality of plaintext segments;  
7       generating the updated key value corresponding to the identified segment and based  
8           on a current key value with forward security and without relying on a key  
9           management process for providing such forward secrecy;  
10       wherein determining another key value based on the current key, the updated key, and  
11           state values that are stored during the generating is computationally infeasible;  
12       and

13 enciphering the plaintext segment by combining the keystream segment with the  
14 segment of the plaintext using a Boolean exclusive OR operation to result in  
15 creating and storing a ciphertext segment.

1 14. A method as recited in Claim 13, wherein each plaintext segment comprises a data  
2 packet conforming to a packet data communication protocol.

1 15. A method as recited in Claim 13, wherein each plaintext segment comprises a data  
2 packet conforming to a packet data communication protocol, and wherein the  
3 enciphering step further comprises encapsulating the data packet according to secure  
4 internet protocol (IPSec).

1 16. A method of encrypting an ordered plurality of packets of a network communication  
2 link using at least an updated key value for a segment of a keystream, with forward  
3 security, the method comprising the computer-implemented steps of:  
4 receiving a packet from among the plurality of packets;  
5 determining a location value that represents a relative location of the packet among  
6 the plurality of packets;  
7 receiving a location value that identifies a location of the segment within the  
8 keystream;  
9 generating the updated key value corresponding to the identified segment and based  
10 on a current key value with forward security and without relying on a key  
11 management process for providing such forward secrecy; and  
12 wherein determining another key value based on the current key, the updated key, and  
13 state values that are stored during the generating is computationally infeasible;  
14 enciphering the packet by combining the keystream segment with data of the packet  
15 using a Boolean exclusive OR operation to result in creating and storing  
16 enciphered packet data.

1 17. A method as recited in Claim 16, wherein the enciphering step further comprises  
2 encapsulating the packet according to secure internet protocol (IPSec).

1 18. A computer-readable medium carrying one or more sequences of instructions for  
 2 automatically generating an updated key value for a segment of keystream for use in a  
 3 cipher, with forward security, which instructions, when executed by one or more  
 4 processors, cause the one or more processors to carry out the steps of:  
 5 receiving a location value that identifies a location of the segment within the  
 6 keystream;  
 7 generating the updated key value corresponding to the identified segment and based  
 8 on a current key value with forward security and without relying on a key  
 9 management process for providing such forward secrecy; and  
 10 wherein determining another key value based on the current key, the updated key, and  
 11 state values that are stored during the generating is computationally infeasible.

1 19. An apparatus for automatically generating an updated key value for a segment of  
 2 keystream for use in a cipher, with forward security, comprising:  
 3 means for receiving a location value that identifies a location of the segment within  
 4 the keystream;  
 5 means for generating the updated key value corresponding to the identified segment  
 6 and based on a current key value with forward security and without relying on  
 7 a key management process for providing such forward secrecy; and  
 8 wherein determining another key value based on the current key, the updated key, and  
 9 state values that are stored during the generating is computationally infeasible.

1 20. An apparatus for automatically generating an updated key value for a segment of  
 2 keystream for use in a cipher, with forward security, comprising:  
 3 a network interface that is coupled to the data network for receiving one or more  
 4 packet flows therefrom;  
 5 a processor;  
 6 one or more stored sequences of instructions which, when executed by the processor,  
 7 cause the processor to carry out the steps of:

8 receiving a location value that identifies a location of the segment within the  
9 keystream;  
10 generating the updated key value corresponding to the identified segment and  
11 based on a current key value with forward security and without relying  
12 on a key management process for providing such forward secrecy; and  
13 wherein determining another key value based on the current key, the updated  
14 key, and state values that are stored during the generating is  
15 computationally infeasible.